IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

1. (Previously Presented) An information reproducing apparatus, comprising:

a hardware secure module having a tamper resistant module structure and storing information related to secure software;

a memory that stores the secure software;

a falsification checking unit that is loaded on the hardware secure module, wherein the falsification checking unit reads the secure software from the memory by direct access without using an operating system, compares the secure software with the information in the hardware secure module, and checks whether the secure software is falsified based on a result of the comparison; and

a processor that executes the secure software when a result of the check by the falsification checking unit is that the secure software is not falsified.

2. (Previously Presented) The information reproducing apparatus according to claim 1, wherein the falsification checking unit reads all of the secure software.

3. (Previously Presented) The information reproducing apparatus according to claim 1, wherein the falsification checking unit reads a part of the secure software.

4. (Previously Presented) The information reproducing apparatus according to claim 1, wherein the falsification checking unit performs the comparison of the information and the secure software using a checksum method.

5. (Cancelled).

6. (Previously Presented) The information reproducing apparatus according to claim 1, wherein the falsification checking unit reads the secure software from the memory on an irregular basis.

7. (Previously Presented) The information reproducing apparatus according to claim 1, further comprising:

a storing unit that is loaded on the hardware secure module and that updates the secure software in the memory using a direct access method.

8. (Previously Presented) The information reproducing apparatus according to claim 7, wherein the storing unit updates the secure software on an irregular basis.

9. (Previously Presented) The information reproducing apparatus according to claim 7, wherein the storing unit updates a part of the secure software.

10. (Previously Presented) The information reproducing apparatus according to claim 7, wherein the falsification checking unit reads the secure software updated by the storing unit.

11. (Previously Presented) The information reproducing apparatus according to claim 7, wherein when the secure software is updated, the storing unit changes over the secure software which has been updated.

12. (Previously Presented) The information reproducing apparatus according to claim 7, wherein the storing unit stores encrypted data in the memory after encryption using a key that exists in the hardware secure module.

13. (Previously Presented) The information reproducing apparatus according to claim 1, further comprising:

a key managing unit that is loaded in the hardware secure module, wherein the key managing unit holds a key used to encrypt or decode data stored in the memory, and the key managing unit outputs the key, if the falsification checking unit does not detect a falsification.

14. (Original) The information reproducing apparatus according to claim 13, wherein the key supplied by the key managing unit is valid only for a predefined period of time.

15. (Previously Presented) The information reproducing apparatus according to claim 13, wherein the key managing unit changes the key each time the key managing unit outputs the key.

16. (Previously Presented) The information reproducing apparatus according to claim 13, wherein when the falsification checking unit detects a falsification, the key managing unit does not output the key.

17. (Previously Presented) The information reproducing apparatus according to claim 1, further comprising:

a writing unit that is loaded in the hardware secure module, wherein the writing unit writes a secret information within the hardware secure module into the memory using the direct access method, wherein

the falsification checking unit checks falsification of the secure software based on response information corresponding to the secret information.

18. (Previously Presented) The information reproducing apparatus according to claim 17, wherein the secret information is stored in a controlled memory space, wherein

the controlled memory space is such that a correct information is read out from the memory space at a first time and an incorrect information is read out at a second time.

19. (Previously Presented) The information reproducing apparatus according to claim 1, wherein the secure software has a function of decoding encrypted MPEG data.

20. (Previously Presented) An information reproducing method comprising:

reading secure software stored in a memory using direct access method without using an operating system, by a hardware secure module having a tamper resistant module structure which stores information related to the secure software;

checking falsification by a falsification checking unit that is loaded on the hardware secure module, by comparing the secure software with the information, and determining whether

the secure software is falsified based on a result of the comparison; and

executing the secure software by a processor when a result of determining is that the secure software is not falsified.

21. (Previously Presented) A hardware secure module mounted to an information reproducing apparatus and having a tamper resistant module structure, comprising:

a reading unit that reads a secure software from a memory mounted to the information reproducing apparatus by direct access without using an operating system; and

a falsification checking unit that compares the secure software with information related to the secure software stored in the hardware secure module, and checks a falsification of the secure software based on a result of the comparison, wherein if the result of the comparison shows that the secure software is not falsified the secure software is executed by the information reproducing apparatus.

22. (Previously Presented) The hardware secure module according to claim 21, wherein the reading unit reads all of the secure software.

23. (Previously Presented) The hardware secure module according to claim 21, wherein the reading unit reads a part of the secure software.

24. (Previously Presented) The hardware secure module according to claim 21, wherein the falsification checking unit performs the comparison of the information and the secure software using a checksum method.

25. (Cancelled).

26. (Previously Presented) The hardware secure module according to claim 21, wherein the reading unit reads the secure software from the memory on an irregular basis.

27. (Previously Presented) The hardware secure module according to claim 21, further comprising:

a storing unit that stores the secure software in the memory using a direct access method.

28. (Previously Presented) The hardware secure module according to claim 27, wherein the storing unit updates the secure software on an irregular basis.

29. (Previously Presented) The hardware secure module according to claim 27, wherein the storing unit updates a part of the secure software.

30. (Previously Presented) The hardware secure module according to claim 27, wherein the falsification checking unit reads the secure software updated by the storing unit.

31. (Previously Presented) The hardware secure module according to claim 27, wherein when the secure software is updated, the storing unit changes over the secure software which has been updated.

32. (Previously Presented) The hardware secure module according to claim 27, wherein the storing unit stores encrypted data in the memory after encryption using a key that exists in the secure module.

33. (Previously Presented) The hardware secure module according to claim 21, further comprising:

a key managing unit that holds a key used to encrypt or decode data stored in the memory, and the key managing unit outputs the key, if the falsification checking unit does not detect a falsification.

34. (Previously Presented) The hardware secure module according to claim 33, wherein the key supplied by the key managing unit is valid only for a predefined period of time.

35. (Previously Presented) The hardware secure module according to claim 33, wherein the key managing unit changes the key each time the key managing unit outputs the key.

36. (Previously Presented) The hardware secure module according to claim 33, wherein when the falsification checking unit detects a falsification, the key managing unit does not output the key.

37. (Previously Presented) The hardware secure module according to claim 21, further comprising:

a writing unit that writes a secret information within the secure module into the memory using the direct access method, wherein

the falsification checking unit determines falsification of the secure software based on response information corresponding to the secret information.

38. (Previously Presented) The hardware secure module according to claim 37, wherein the secret information is stored in a controlled memory space, wherein the controlled memory space is such that a correct information is read out from the memory space at a first time and an incorrect information is read out at a second time.

39. (Previously Presented) The hardware secure module according to claim 21, wherein the secure software has a function of decoding encrypted MPEG data.

40. (Previously Presented) A recording medium that records a program for causing a hardware secure module mounted to an information reproducing apparatus to execute a process, the process comprising:

reading secure software stored in a memory using a direct access method and without using an operating system, by the hardware secure module having a tamper resistant module structure storing information related to the secure software;

checking falsification by comparing the secure software with the first information, and determining a falsification of the secure software based on a result of the comparison; and

executing the secure software when the result of the comparison is that the secure software is not falsified.

41. (Previously Presented) A method of a reproducing verified information, comprising:

executing secure software that is stored in a memory accessible to an information reproducing apparatus using a direct access method, if comparison of the secure software with information related to the secure software stored in a hardware secure module having a tamper resistant module structure inaccessible from outside, indicates that the secure software is not falsified.